(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－171510
（P2002－171510A）
(43)公開日　平成14年６月14日(2002.6.14)

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04N 7/173	610	H04N 7/173	610Z 5C025
5/44		5/44	A 5C064
			Z

審査請求　未請求　請求項の数９　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－367832(P2000－367832)

(22)出願日　平成12年12月１日(2000.12.1)

(71)出願人　000006079
ミノルタ株式会社
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル

(72)発明者　原　吉宏
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内

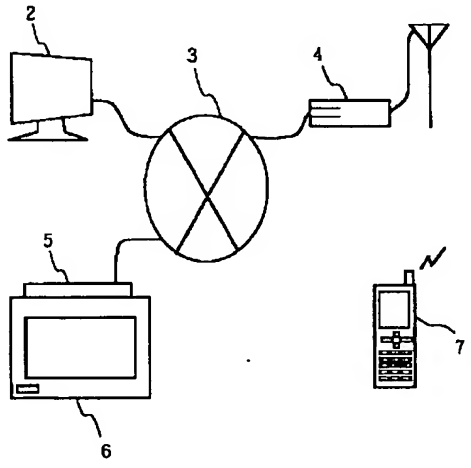
(72)発明者　出山　弘幸
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内

(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　画像サーバ装置、当該画像サーバ装置を用いた画像通信システム

(57)【要約】
【課題】　デジタル画像をサーバ装置に格納すると、必要な範囲に自動的にその旨を通知する画像通信システムを提供する。
【解決手段】　画像データを格納する複数の記憶領域を有する記憶装置を備えた画像サーバ装置４と端末２、５、７をネットワーク接続した画像通信システムにおいて、画像サーバ装置４は、画像データを格納する少なくとも１の記憶領域を有する記憶装置と、画像データの前記記憶装置への格納を要求する格納要求であって、当該画像データを格納する記憶領域を指定する領域指定を含む格納要求を提供端末から受け付ける格納要求受付手段と、領域指定により指定された記憶領域に画像データを書き込む書き込み手段と、画像データを格納した旨を通知する格納通知の宛先となる表示端末を、前記領域指定を用いて決定する宛先決定手段と、宛先決定手段により決定された宛先に、格納通知を送信する格納通知手段とを備える。



【特許請求の範囲】
【請求項１】　ネットワークを介して接続される端末装置に対して、閲覧属性に応じて画像データの参照を許可する画像サーバ装置であって、
閲覧属性を付与して画像データを記憶する記憶手段と、
閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付手段と、
画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定手段と、
決定された宛先に前記記憶通知を送信する記憶通知手段とを備えることを特徴とする画像サーバ装置。
【請求項２】　閲覧属性に対応する記憶領域を決定する記憶領域決定手段を備え、
前記記憶手段は、決定された記憶領域に画像データを記憶することを特徴とする請求項１に記載の画像サーバ装置。
【請求項３】　前記各記憶領域に対応付けて第１の認証情報を記憶する第１の認証情報記憶手段と、
前記端末装置から画像データの参照を要求する第１の参照要求を受け付ける第１の参照要求受付手段と、
前記決定された宛先以外の端末装置から前記第１の参照要求を受け付けた場合、要求された画像データを記憶する記憶領域に対応付けられた第１の認証情報と当該端末装置から受け付けた第２の認証情報とを照合して、画像データの参照を許可するかどうかを決定する参照許可手段とを備えることを特徴とする請求項２に記載の画像サーバ装置。
【請求項４】　メッセージを含む前記記憶要求を受け付けるメッセージ付き記憶要求受付手段と、
前記記憶要求に係る画像データに関連付けて前記メッセージを記憶するメッセージ記憶手段と、
当該記憶要求に係る画像データの参照を端末装置から要求されると、当該記憶要求に含まれたメッセージを返信するメッセージ返信手段を備えることを特徴とする請求項３に記載の画像サーバ装置。
【請求項５】　前記メッセージを返信された端末装置から返信メッセージを受け付ける返信メッセージ受付手段と、
前記メッセージに関連付けて前記返信メッセージを記憶する返信メッセージ記憶手段と、
受け付けた返信メッセージを、前記メッセージを含む記憶要求の要求元である端末装置に転送する返信メッセージ転送手段を備えることを特徴とする請求項４に記載の画像サーバ装置。
【請求項６】　画像データを提供する画像提供端末、画像データを表示する画像表示端末、および請求項１に記載の画像サーバ装置をネットワーク接続した画像通信システムであって、
画像提供端末は、画像サーバ装置に記憶要求を送信する記憶要求手段を備え、
画像表示端末は、画像サーバ装置から記憶通知を受信する通知受信手段と、
記憶通知を受信した旨を表示する通知表示手段とを備えることを特徴とする画像通信システム。
【請求項７】　前記画像サーバ装置は、記憶要求に係る画像データの指定と閲覧属性とを記憶する指定情報記憶手段と、
記憶通知に係る画像データの参照を要求する第２の参照要求を表示端末から受け付ける第２の参照要求受付手段と、
第２の参照要求を送信した表示端末に当該要求に係る画像データを返信する画像データ返信手段とを備え、
前記表示端末は、第２の参照要求を送信する第２の参照要求手段と、
第２の参照要求に対して返信された画像データを画像サーバ装置から受信する画像データ受信手段とを備えることを特徴とする請求項６に記載の画像通信システム。
【請求項８】　端末装置に対して閲覧属性に応じて画像データの参照を許可する画像サーバ装置と、端末装置とをネットワーク接続した画像通信システムにおいて、
閲覧属性を付与して画像データを記憶する記憶ステップと、
閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付ステップと、
画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定ステップと、
決定された宛先に記憶通知を送信する記憶通知ステップとを前記画像サーバ装置に実行させることを特徴とする画像通信方法。
【請求項９】　請求項８に記載の画像通信方法を画像サーバ装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は画像データを格納するサーバ装置とネットワークを介して当該サーバ装置に画像データに格納したり、格納された画像データを参照したりする端末装置からなる画像通信システムに関し、特に画像データに対する端末装置からのアクセスをサーバ装置に管理させる画像通信システムに関する。
【０００２】
【従来の技術】近年、パソコンやデジタルカメラ等の普及によりデジタル画像が非常に身近なものとなってきている。デジタル画像はインターネット等のネットワークを介して容易に伝送することができるため、サーバ装置にデジタル画像を蓄えて、端末装置（パソコン、携帯電

話等）から参照させる画像通信システムが盛んに利用されている。例えば、ネットワークを介して投稿されたデジタル画像をホームページにて参照させるサービスが提供されており、このようなシステムでは不特定多数の利用者がデジタル画像を発表したり、参照したりすることができる。

【０００３】このようなサービスを利用してデジタル画像を参照する場合、新規なデジタル画像が投稿されたかどうかを予め知ることができないため、サーバ装置に空しく何度もアクセスして、新規なデジタル画像が投稿されていないことを確認する破目となることもしばしばである。これに対して、例えば特開２０００－２０３７１号公報に開示の情報ライブラリー・サーバー／クライアントシステムは、情報ライブラリー・サーバーに新規に登録された情報ファイルに添付された情報タイトルと、情報タイトルと通知先グループを対応付ける登録情報・通知情報ファイルと、各通知先グループ名に属する通知先を定義した通知先グループテーブルとを参照して、情報ファイルが新規に登録された旨を通知する通知先を決定することによって当該通知先に先の旨を通知するというものである。

【０００４】このようにすれば、新規に情報ファイルが登録されたことが通知されるので、徒らに情報ライブラリー・サーバーにアクセスすることを回避できる。

【０００５】

【発明が解決しようとする課題】近年、情報システムにおけるセキュリティの強化が強く求められており、情報ファイルについてもアクセス権を設定する必要がある。これに対して上記の従来技術は情報ファイルに対するアクセス権に関わらず前記通知を行うため、情報ファイルの新規登録を通知された者がアクセス権の制限により当該情報ファイルを参照できない場合がある。

【０００６】この問題を解消するには前記通知先グループ・テーブルに通知先グループ毎の通知先を設定する際に情報ファイルに対するアクセス権を考慮する必要があるのだが、情報ファイルに対するアクセス権に設定が変更されるたびに通知先の設定を変更することは極めて煩瑣な作業であるし、そもそもアクセス権を考慮して通知先を設定すること自体が困難である。

【０００７】本発明は、上記のような問題に鑑みてなされたものであって、デジタル画像をサーバ装置に格納すると、当該デジタル画像に関するアクセス権に応じて格納を通知する画像通信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明に係る画像サーバ装置は、ネットワークを介して接続される端末装置に対して、閲覧属性に応じて画像データの参照を許可する画像サーバ装置であって、閲覧属性を付与して画像データを記憶する記憶手段と、閲覧属性を指定して前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付手段と、画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定手段と、決定された宛先に前記記憶通知を送信する記憶通知手段とを備えることを特徴とする。このようにすれば、デジタル画像をサーバ装置に格納するだけで、当該デジタル画像に関するアクセス権に応じて当該デジタル画像の格納を通知させることができる。

【０００９】また、閲覧属性に対応する記憶領域を決定する記憶領域決定手段を備え、前記記憶手段は、決定された記憶領域に画像データを記憶することを特徴とする。また、前記各記憶領域に対応付けて第１の認証情報を記憶する第１の認証情報記憶手段と、前記端末装置から画像データの参照を要求する第１の参照要求を受け付ける第１の参照要求受付手段と、前記決定された宛先以外の端末装置から前記第１の参照要求を受け付けた場合、要求された画像データを記憶する記憶領域に対応付けられた第１の認証情報と当該端末装置から受け付けた第２の認証情報とを照合して、画像データの参照を許可するかどうかを決定する参照許可手段とを備えることを特徴とする。

【００１０】また、メッセージを含む前記記憶要求を受け付けるメッセージ付き記憶要求受付手段と、前記記憶要求に係る画像データに関連付けて前記メッセージを記憶するメッセージ記憶手段と、当該記憶要求に係る画像データの参照を端末装置から要求されると、当該記憶要求に含まれたメッセージを返信するメッセージ返信手段を備えることを特徴とする。このようにすれば、デジタル画像に併せて、当該デジタル画像に関するメッセージを伝達させることができる。

【００１１】また、前記メッセージを返信された端末装置から返信メッセージを受け付ける返信メッセージ受付手段と、前記メッセージに関連付けて前記返信メッセージを記憶する返信メッセージ記憶手段と、受け付けた返信メッセージを、前記メッセージを含む記憶要求の要求元である端末装置に転送する返信メッセージ転送手段を備えることを特徴とする。このようにすれば、前記メッセージに対する応答のメッセージを返信することができるので、特定のデジタル画像をトピックスとしてユーザ間のコミュニケーションを図ることができる。

【００１２】また、本発明に係る画像通信システムは、画像データを提供する画像提供端末、画像データを表示する画像表示端末、および請求項１に記載の画像サーバ装置をネットワーク接続した画像通信システムであって、画像提供端末は、画像サーバ装置に記憶要求を送信する記憶要求手段を備え、画像表示端末は、画像サーバ装置から記憶通知を受信する通知受信手段と、記憶通知を受信した旨を表示する通知表示手段とを備えることを特徴とする。

【００１３】また、前記画像サーバ装置は、記憶要求に係る画像データの指定と閲覧属性とを記憶する指定情報記憶手段と、記憶通知に係る画像データの参照を要求する第２の参照要求を表示端末から受け付ける第２の参照要求受付手段と、第２の参照要求を送信した表示端末に当該要求に係る画像データを返信する画像データ返信手段とを備え、前記表示端末は、第２の参照要求を送信する第２の参照要求手段と、第２の参照要求に対して返信された画像データを画像サーバ装置から受信する画像データ受信手段とを備えることを特徴とする。

【００１４】また、本発明に係る画像通信方法は、端末装置に対して閲覧属性に応じて画像データの参照を許可する画像サーバ装置と、端末装置とをネットワーク接続した画像通信システムにおいて、閲覧属性を付与して画像データを記憶する記憶ステップと、閲覧属性を指定して、前記記憶手段に画像データを記憶させることを要求する記憶要求を受け付ける記憶要求受付ステップと、画像データを記憶した旨を通知する記憶通知の宛先となる端末装置を閲覧属性に基づいて決定する宛先決定ステップと、決定された宛先に記憶通知を送信する記憶通知ステップとを前記画像サーバ装置に実行させることを特徴とする。

【００１５】また、本発明に係る記録媒体は、コンピュータ読み取り可能な記録媒体であって、前記画像通信方法を画像サーバ装置に実行させるプログラムが記録されている。

【００１６】

【発明の実施の形態】以下、本発明に係る画像通信システムの実施の形態を、図面を参照しながら説明する。

（実施の形態）図１は、本発明に係る画像通信システム１を示した図である。画像通信システム１は、一家庭内に敷設されたホームネットワーク３にホームサーバ４、パーソナルコンピュータ２、テレビ受像機６が接続されており、更にホームサーバ４は公衆回線を介して随時、携帯電話７に接続される。パーソナルコンピュータ２、ホームサーバ４、テレビ受像機６は互いにＴＣＰ／ＩＰ（Transmission ControlProtocol/Internet Protocol）を用いてデジタル画像等のデータを交換する。

【００１７】なお、テレビ受像機６にはセットトップボックス５が搭載されており、当該セットトップボックス５を介してホームネットワーク３に接続されている。セットトップボックス５は、外部インタフェースとしてアンテナ端子、ビデオ出力端子等を備え、また、チューナを内蔵している。前記アンテナ端子にはテレビアンテナが接続されている。前記ビデオ出力端子はテレビ受像装置のビデオ入力端子に接続されており、セットトップボックス５が前記チューナにて受信したテレビ映像をテレビ受像装置に表示させる。また、セットトップボックス５はシリアルポートを有しており、当該ポートにデジタルカメラ等を接続して、デジタル画像を電子ファイル（例えば、ＭＰＥＧファイル）の形式で、セットトップボックス５に内部記憶装置に格納させることができる。

【００１８】図２は、前記セットトップボックス５に付属のリモートコントローラを示した図である。セットトップボックス５は不図示の赤外線ポートを有しており、リモートコントローラ１０は赤外線ポート１６を用いて、セットトップボックス５と通信する。リモートコントローラ１０は、電源ボタン１１、チャンネルボタン１７等を備えており、電源ボタン１１はセットトップボックス５の電源をオンオフさせるためのボタンである。チャンネルボタン１７は、テレビ受像装置に表示させるチャンネルを選択するためのボタンであり、後述のようにテキスト入力にも用いる。テレビボタン１８は、テレビ受像装置にテレビ番組を表示させるために用いるボタンである。カーソルキー１２～１５、およびボタン１９～２１の機能については後述する。

【００１９】さて、画像通信システム１の利用者は、パーソナルコンピュータ２に格納されたデジタル画像を、次のようにしてホームサーバ４に格納させる。まず、パーソナルコンピュータ２においてブラウザを起動し、ホームサーバ４のＷｅｂページを表示させる。図３は、ホームサーバ４のエントリ画面に相当するＷｅｂページである。エントリ画面３０には、タイトル文字３１、ホームサーバ４に格納されたデジタル画像を参照するための参照ボタン３２、およびホームサーバ４にデジタル画像を格納するための登録ボタン３３が表示される。

【００２０】利用者が登録ボタン３３をクリックすると、格納すべきデジタル画像の電子ファイル名を入力させるウィンドウ、すなわち登録画面が表示される。図４は、デジタル画像をホームサーバ４の記憶装置に格納させるための登録画面である。登録画面４０には、デジタル画像を格納するホームサーバ内のフォルダを指定させるテキストボックス４１、ホームサーバ４の記憶装置に格納させるデジタル画像を表示させる画像表示エリア４２、デジタル画像とともにホームサーバに送付するメッセージを入力させるテキストボックス４３、および登録ボタン４４が配されている。

【００２１】利用者は、テキストボックス４１、４３へはキーボードを用いてテキストを入力し、デジタル画像の指定についてはファイルマネージャ等からデジタル画像を格納した電子ファイルを画像表示エリア４２にドラッグして表示させることにより行う。登録ボタン４４は、テキストボックス４１、４３への入力が完了した後にクリックされるボタンであって、当該登録ボタン４４がクリックされると、テキストボックス４１、４３に入力された内容と画像表示エリア４２に表示されたデジタル画像データが、ホームサーバ４に送付される。

【００２２】また、画像通信システム１の利用者は、前記セットトップボックス５の内部記憶装置に格納されたデジタル画像をホームサーバ４に格納させる場合には、

次のようにする。リモートコントローラ１０の画像ボタン１９が押下されると、テレビ受像機６にホームサーバ４のエントリ画面３０が表示される。ここで、カーソルキー１２～１５を操作して登録ボタン３３を選択し、リモートコントローラ１０の完了ボタン２１を押下すると、今度はテレビ受像機６に登録画面４０が表示される。カーソルキー１２～１５を操作してテキストボックス４１を選択し、リモートコントローラ１０の表示ボタン１９を押下すると、フォルダ名を列挙したプルダウンメニューが表示される。利用者は、更にカーソルキー１２～１５を操作して、プルダウンメニューに表示されたフォルダのうち、デジタル画像を格納したいフォルダを反転表示させたのち、リモートコントローラ１０の完了ボタン２１を押下すると、反転表示させたフォルダ名がテキストボックス４１に入力される。

【００２３】デジタル画像の指定については、まず画像表示エリア４２を選択した後、表示ボタン２０を押下すると、画像表示エリア４２にデジタル画像が表示される。この時、カーソルキー１２～１５を操作すると、セットトップボックス５の内部記憶装置に格納されたデジタル画像が順に画像表示エリア４２に表示されるので、ホームサーバ４に格納したいデジタル画像を表示させた後、完了ボタン２１を押下すると、当該デジタル画像が選択される。

【００２４】メッセージについては、テキストボックス４３を選択した後、チャンネルボタン１７を用いて、テキストボックス４３に入力する。これらの入力が完了したら、更にカーソルキー１２～１５を操作して登録ボタン４４を選択し、完了ボタン２１を押下すると、テキストボックス４１、４３に入力された内容と画像表示エリア４２に表示されたデジタル画像が、ホームサーバ４に送付される。すなわち、ホームサーバ４に対する格納要求として、デジタル画像を格納する領域を指定するフォルダ名、デジタル画像、およびメッセージが送信される。

【００２５】次に、ホームサーバ４について説明する。ホームページ４は、大容量の内部記憶装置を備えており、当該内部記憶装置にはデジタル画像を格納する複数のフォルダと、各端末装置からの格納されたデジタル画像に対するアクセスをフォルダ毎に管理するアクセス管理テーブルを備えている。図５は、アクセス管理テーブルを例示した図である。図５のアクセス管理テーブルには、利用者の家族構成（父、母、長男、次男、長女）に合わせた、共用フォルダ、パパ用フォルダ、ママ用フォルダ、太郎用フォルダ、次郎用フォルダ、花子用フォルダの計６つのフォルダに対する端末装置（パーソナルコンピュータ２、テレビ受像機６、携帯電話７）からのアクセスの可否に関する情報が設定されている。

【００２６】アクセス管理テーブルにおいて、アクセスに可否についての設定「Ａ」は、端末装置からフォルダに対して当該フォルダに格納されたデジタル画像を参照する要求があると、ホームサーバ４は無条件に許可すべきことを意味する。設定「Ｂ」は、端末装置からフォルダに対して当該フォルダに格納されたデジタル画像の参照要求があると、ホームサーバ４は端末装置に対してパスワードを要求し、正しいパスワードが入力された時のみアクセスを許可すべきことを意味する。設定「Ｃ」は、端末装置からフォルダに対してデジタル画像の参照要求があると、ホームサーバ４は無条件に拒絶すべきことを意味する。なお、端末装置からフォルダに対してデジタル画像を格納する要求がきた場合には、ホームサーバ４はアクセス管理テーブルを参照せず、無条件にこれを許可する。

【００２７】因みに、図５のアクセス管理テーブルにおいて、パーソナルコンピュータ２またはテレビ受像機６から共用フォルダに格納されたデジタル画像を参照する場合には無条件に許可されるように、またそれらの端末装置から共用フォルダ以外のフォルダに格納されたデジタル画像を参照する場合には、各フォルダに割り当てられたパスワードを入力するような設定となっている。また、携帯電話７は屋外に持ち出す都合上、セキュリティ確保のために、共用フォルダに格納されたデジタル画像を参照する場合のみパスワードの入力を条件としてアクセスを許可し、共用フォルダ以外のフォルダに格納されたデジタル画像については無条件にアクセスを禁止する設定としている。

【００２８】さて、前述のように各端末装置からホームサーバ４に対してデジタル画像の格納要求が発せられると、ホームサーバ４は当該要求に従ってデジタル画像とメッセージを所定のフォルダに格納する。図６は、端末装置からデジタル画像の格納要求を受信したホームサーバ４の動作を示したフローチャートである。ホームサーバ４は、デジタル画像を指定されたフォルダに格納すると（ステップＳ１）、アクセス管理テーブルの当該フォルダに対応する列を参照して、各端末装置について順に設定を参照する。すなわち、アクセス管理テーブル中で設定を未参照の端末装置を検索して（ステップＳ２）、そのような端末装置を発見したら（ステップＳ３でＹＥＳ）、設定を参照する（ステップＳ４）。この設定が上記「Ａ」、「Ｂ」、「Ｃ」の各設定のうちの「Ａ」であれば（ステップＳ５でＹＥＳ）、当該端末装置にフォルダに新規なデジタル画像を格納した旨の通知、すなわち格納通知を送付する（ステップＳ６）。ステップＳ４で参照した設定が「Ｂ」または「Ｃ」ならば（ステップＳ５でＮＯ）、ステップＳ２に進んで再び設定を未参照の端末装置を検索する。そうして、未参照の端末装置が見つからなければ（ステップＳ３でＮＯ）、処理を終了する。なお、ホームサーバ４は、デジタル画像を記憶装置に格納する際に、当該デジタル画像の格納を要求した端末装置の識別情報を登録元情報として併せて格納する。

【００２９】次に、端末装置からホームサーバ４の記憶装置に格納されたデジタル画像を参照する際の処理について、セットトップボックス５、パーソナルコンピュータ２、携帯電話７の順に説明する。ホームサーバ４の記憶装置に格納されたデジタル画像をテレビ受像機６に表示させるために、利用者はセットトップボックス５を次のように操作する。図７は、デジタル画像をテレビ受像機６に表示させるための典型的な操作手順を示したフローチャートである。利用者は、先ずリモートコントローラ１０を操作してセットトップボックス５の電源を投入する（ステップＳ１０）。次に、画像ボタン１９を押下してテレビ受像機６にエントリ画面３０を表示させ（ステップＳ１１）、当該エントリ画面３０中の参照ボタン３２をクリックする（ステップＳ１２）。なお、参照ボタン３２のクリックの仕方については、上述した登録ボタン３３のクリックの仕方と同様である。利用者が登録ボタン３３をクリックすると、テレビ受像機６に参照画面が表示される。

【００３０】図８は、デジタル画像の電子ファイル名を入力させるための参照画面である。参照画面５０には、表示させたいデジタル画像を格納したホームサーバ内のフォルダを指定させるテキストボックス５１、デジタル画像を表示させる画像表示エリア５２、デジタル画像とともにホームサーバに格納されているメッセージを表示させるテキストボックス５３、前記メッセージに対する返信メッセージを入力させるテキストボックス５４、および返信ボタン５５が配されている。

【００３１】利用者は、リモートコントローラ１０のカーソルキー１２～１５を操作してテキストボックス５１を選択し、リモートコントローラ１０の表示ボタン１９を押下すると、フォルダ名を列挙したプルダウンメニューが表示される。利用者は、更にカーソルキー１２～１５を操作して、プルダウンメニューに表示されたフォルダのうち、所望のフォルダを反転表示させたのち、リモートコントローラ１０の完了ボタン２１を押下すると、反転表示させたフォルダ名がテキストボックス５１に表示される（ステップＳ１３）。

【００３２】完了ボタン２１が押下されると、端末装置名（セットトップボックス５）とフォルダ名を伴って、その旨の通知がセットトップボックス５からホームサーバ４になされる。するとホームサーバ４は、通知された端末装置名とフォルダ名に対応する前記アクセス管理テーブルの設定を参照して、当該設定が「Ｂ」ならば、セットトップボックス５を介してテレビ受像機６にパスワードを要求するウィンドウを表示させる。利用者は、このようにしてパスワードを要求されると（ステップＳ１４でＹＥＳ）、当該ウィンドウにパスワードを入力する（ステップＳ１５）。

【００３３】すると、当該パスワードがホームサーバ４に転送される。ホームサーバ４は、受信したパスワードと記憶装置に保存されているパスワードとを照会して一致したら、アクセスを許可する旨のメッセージを表示するウィンドウをテレビ受像機６に表示させる。受信したパスワードが正しくなければ、アクセスを拒絶する旨のメッセージを表示するウィンドウをテレビ受像機６に表示させる。

【００３４】利用者は、パスワードを要求されなければ（ステップＳ１４でＮＯ）、またはホームサーバ４によりアクセスを許可されたら、参照画面５０上で画像表示エリア５２を選択した後、表示ボタン２０を押下すると、画像表示エリア５２にデジタル画像が表示される。この時、カーソルキー１２～１５を操作すると、セットトップボックス５の内部記憶装置に格納されたデジタル画像が順に画像表示エリア５２に表示される（ステップＳ１６）。

【００３５】このとき同時に、画像表示エリア５２に表示されたデジタル画像がホームサーバ４に格納された時に併せて格納されたメッセージがテキストボックス５３に表示される。利用者が当該メッセージに対して応答したい場合には（ステップＳ１７でＹＥＳ）、登録画面でメッセージを入力したのと同様の手順で、テキストボックス５４に返信メッセージを入力した後（ステップＳ１８）、返信ボタン５５をクリックすると（ステップＳ１９）、テキストボックス５４に入力した返信メッセージがホームサーバ４に送付される。なお、返信メッセージにはテキストボックス５１に表示されたフォルダ名と画像表示エリアに表示されたデジタル画像の識別子が自動的に添付されている。また、デジタル画像の識別子は当該デジタル画像をホームサーバ４が端末装置に送付する時に自動的に添付される。

【００３６】本発明に係る画像通信システム１を用いて、ホームサーバ４の記憶装置に格納されたデジタル画像をテレビ受像機６に表示させる場合、上記のほかに次のような操作手順も許される。セットトップボックス５はホームサーバ４から上述の格納通知を受信すると、テレビ受像機６に格納通知を受信した旨のメッセージをテロップ（TELOP: Television Opaque Projector）表示させる。このテロップ表示は所定時間（１０秒間）だけ継続し、その後、自動的にテロップ表示を終了する。当該テロップが表示されている期間中に利用者がリモートコントローラ１０の画像ボタン１９を押下すると、その旨がセットトップボックス５からホームサーバ４に直ちに通知され、通知を受けたホームサーバ４はテレビ受像機６に参照画面５０を表示させる。この時、参照画面５０のテキストボックス５１、５３には自動的にフォルダ名とメッセージが、画像表示エリア５２には自動的にデジタル画像が表示される。このようにすれば、格納通知を受信した際に、簡単な手順で新規に追加されたデジタル画像を参照することができる。

【００３７】なお、ホームサーバ４は、端末装置に格納

通知を送信する際に、当該格納通知に係る諸情報（デジタル画像、メッセージ、格納を要求した端末装置等）を端末装置毎に格納通知テーブルに格納しており、上記のように格納通知に係るデジタル画像の参照を端末装置から要求されると、当該格納通知テーブルを参照して最後に送信した格納通知に係るデジタル画像の参照を要求した端末装置に返信する。また、このとき格納通知テーブルにメッセージが格納されていたら、当該メッセージも併せて端末装置に返信する。

【００３８】テレビ受像機６に代えてパーソナルコンピュータ２を用いて、ホームサーバ４に格納されたデジタル画像を参照する手順についても概ね同様であるが、テレビ受像機６の場合におけるテロップ表示については、特に次に述べるようにする。すなわち、ホームサーバ４からの格納通知を受信して、格納通知を受信した旨をパーソナルコンピュータ２の表示画面上にポップアップ表示させるプログラムをパーソナルコンピュータ２に常駐させて、以下の処理を遂行させる。

【００３９】図９は、当該常駐プログラムがパーソナルコンピュータ２の表示画面上にポップアップ表示させるポップアップウィンドウを示した図である。パーソナルコンピュータ２の常駐プログラムはホームサーバ４から格納通知を受信すると図９のような格納通知画面を表示したポップアップウィンドウを表示する。格納通知画面にはホームサーバ４に新規なデジタル画像が登録された旨のメッセージ６１と、当該デジタル画像を参照させるための参照ボタン６２が表示されている。

【００４０】パーソナルコンピュータ２の利用者が前記参照ボタン６２をクリックすると、その旨がパーソナルコンピュータ２からホームサーバ４に直ちに通知され、通知を受けたホームサーバ４はパーソナルコンピュータ２に参照画面５０を表示させる。この時、参照画面５０のテキストボックス５１、５３には自動的にフォルダ名とメッセージが、画像表示エリア５２には自動的にデジタル画像が表示される。このようにすればテレビ受像機の場合と同様にして、格納通知を受信した際に、簡単な手順で新規に追加されたデジタル画像を参照することができる。

【００４１】さて、端末装置（パーソナルコンピュータ２またはセットトップボックス５）から返信メッセージを受信したホームサーバ４は、返信メッセージに添付されたフォルダ名とデジタル画像の識別子を用いて記憶装置に格納されたデジタル画像を特定し、特定したデジタル画像に付随して記憶装置に格納されている当該デジタル画像の登録元情報を参照し、前記返信メッセージを当該デジタル画像の登録元に転送する。

【００４２】セットトップボックス５は、ホームサーバ４から返信メッセージを受信すると、その旨を示すテロップをテレビ受像機に表示させる。このテロップ表示は、格納通知を受信した旨のテロップと同様に、所定時間（１０秒間）だけ継続した後、自動的に終了する。当該テロップが表示されている期間中に利用者がリモートコントローラ１０の画像ボタン１９を押下すると、その旨がセットトップボックス５からホームサーバ４に直ちに通知され、通知を受けたホームサーバ４はテレビ受像機６に返信メッセージ参照画面を表示させる。図１０は、返信メッセージ参照画面を示した図である。返信メッセージ参照画面７０の画像表示エリア７１にはデジタル画像が、テキストボックス７２、７３には返信メッセージと当該返信メッセージの発信元端末装置の名称がそれぞれ表示される。

【００４３】パーソナルコンピュータ２がホームサーバ４から返信メッセージを受信する場合については、前記格納通知を受信する場合と同様に、パーソナルコンピュータ２に常駐する常駐プログラムが返信メッセージを受信して、図１０と同様の返信メッセージ参照画面を表示したポップアップウィンドウを表示する。以上のようにすれば、ホームサーバ４に新規なデジタル画像を登録した際に、当該デジタル画像に関連する端末装置にのみ自動的にその旨が通知されるので、新規デジタル画像がホームサーバ４に格納されたかどうかをチェックするために端末装置から頻繁に参照しにゆくという無駄な手間を省くことができるのみならず、各利用者による端末装置の占有時間を低減させて端末装置の利用効率を高めることができるので、ネットワークの負荷や電力消費等を低減させることができる。

（変形例）以上、本発明を実施の形態に基づいて説明してきたが、本発明は、上述の実施の形態に限定されないのは勿論であり、以下のような変形例を実施することができる。

【００４４】上記実施の形態においては、アクセス管理テーブルでの設定が「Ｂ」の場合、必ずパスワードを問い合わせるとしたが、パーソナルコンピュータ２のようにログイン時にパスワード等により認証を行う端末装置については、次のようにしてパスワードの問い合わせをスキップするとしてもよい。図１１は、本変形例に係る画像通信システムのホームサーバに格納されたアクセス管理テーブルを示した図である。当該アクセス管理テーブルが上記実施の形態に係るアクセス管理テーブルと異なる点は、パーソナルコンピュータ２からのアクセスについての設定がすべて「Ａ」となっている点である。パーソナルコンピュータはログイン時にパスワードを要求するので、このように設定してパスワードの入力回数を削減してもセキュリティを保つことができる。

【００４５】また、図１２は、このような機能を有するアクセス管理テーブルの別の変形例である。図１２のアクセス管理テーブルは、端末装置毎にタイプ設定欄を設けて、パスワードの要、不要を設定させる。前記のようにログイン時等に認証を行う端末装置については当該タイプ設定欄に「フリー」と設定して、ホームサーバ４か

らのパスワードの問い合わせが不要である旨を表示し、タイプ設定欄に「チェック」と設定されている端末装置にのみホームサーバ４からパスワードの問い合わせを行わせる。

【００４６】このようにすれば、パスワード等、認証情報を入力する回数を低減することができるので操作性をより高めることができる。なお、本発明は、上記に示す方法であるとしてもよいし、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよい。また、当該コンピュータプログラムをコンピュータ読み取り可能な記録媒体（フロッピー（登録商標）ディスク、ハードディスク、ＣＤ－ＲＯＭ等）に記録したものとしてもよい。

【００４７】

【発明の効果】以上説明したように、本発明によれば、サーバ装置に新規デジタル画像を格納させる際に、その旨を自動的に所定の端末装置に通知させるので、新規画像が登録されていないことを確認するだけに終わるような無駄なアクセスを無くすことができる。したがって、サーバ装置に無駄にアクセスして落胆するような事態を回避できると共に、無駄なアクセスに伴って生じる電力やネットワーク資源の消費を低減することができる。

【００４８】また、上記の通知を受ける端末装置を設定により予め指定できるので、そのような通知を必要としない端末装置に対して通知がなさることがない。したがって、通知の乱発によって通信等のログが急速に増大するような事態を回避できるので、当該ログの格納に費消されるサーバ装置や端末装置の固定記憶装置等の記憶容量を節約することができる。

【００４９】更に、上記通知がなされた折には、デジタル画像の参照要求に対して自動的に当該通知に係るデジタル画像を端末装置に表示させるので、新規に格納されたデジタル画像を探し回る手間を省きく、速やかに表示させることができる。したがって、そのような探し回りに伴う煩わしさを去り、画像通信システムの利用効率を向上させることができる。

【図面の簡単な説明】

【図１】本発明に係る画像通信システム１を示した図である。

【図２】セットトップボックス５に付属のリモートコントローラを示した図である。

【図３】ホームサーバ４のエントリ画面に相当するＷｅｂページである。

【図４】デジタル画像をホームサーバ４の記憶装置に格納させるための登録画面である。

【図５】アクセス管理テーブルを例示した図である。

【図６】端末装置からデジタル画像の格納要求を受信したホームサーバ４の動作を示したフローチャートである。

【図７】デジタル画像をテレビ受像機６に表示させるための典型的な操作手順を示したフローチャートである。

【図８】デジタル画像の電子ファイル名を入力させるための参照画面である。

【図９】常駐プログラムがパーソナルコンピュータ２の表示画面上にポップアップ表示させるポップアップウィンドウを示した図である。

【図１０】返信メッセージ参照画面を示した図である。

【図１１】変形例に係る画像通信システムのホームサーバ４に格納されたアクセス管理テーブルを示した図である。

【図１２】変形例に係る画像通信システムのホームサーバ４に格納されたアクセス管理テーブルを示した図である。

【符号の説明】

１　画像通信システム
２　パーソナルコンピュータ
３　ホームネットワーク
４　ホームサーバ
５　セットトップボックス
６　テレビ受像機
７　携帯電話
１０　リモートコントローラ
１１　電源ボタン
１２～１５　カーソルキー
１６　赤外線ポート
１７　チャンネルボタン
１８　テレビボタン
１９　画像ボタン
２０　表示ボタン
２１　完了ボタン

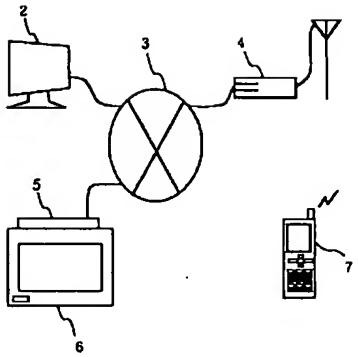
【図５】

端末装置	フォルダ					
	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	A	B	B	B	B	B
テレビ受像機	A	B	B	B	B	B
携帯電話	B	C	C	C	C	C

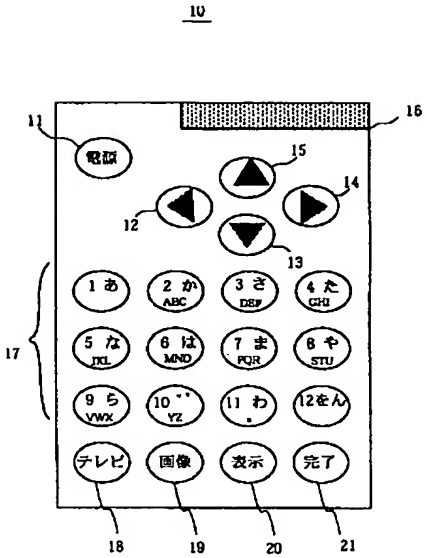
【図１１】

端末装置	フォルダ					
	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	A	A	A	A	A	A
テレビ受像機	A	B	B	B	B	B
携帯電話	B	C	C	C	C	C

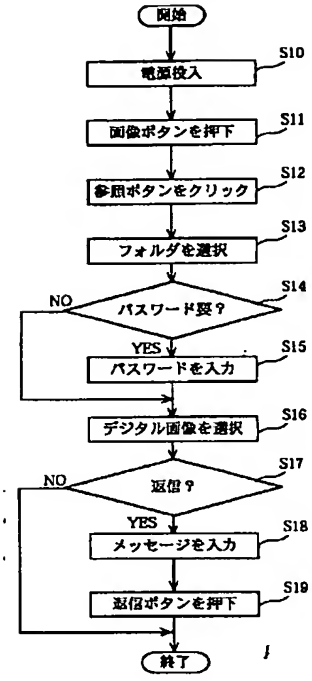
【図１】



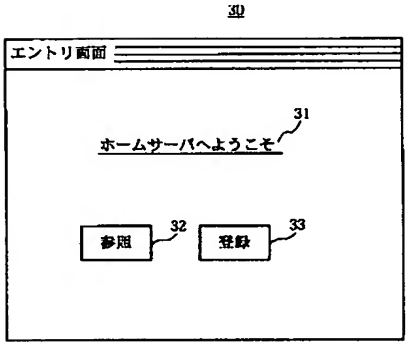
【図２】



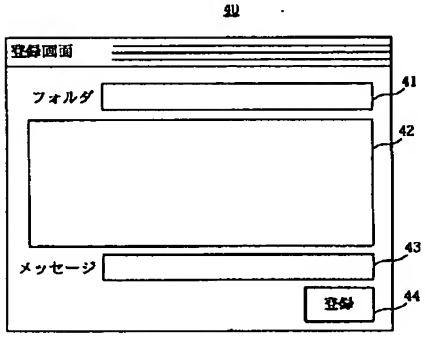
【図７】



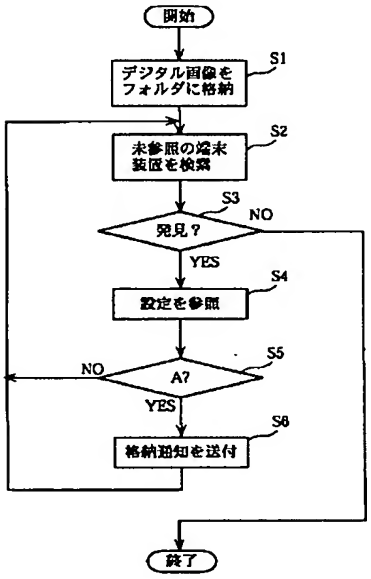
【図３】



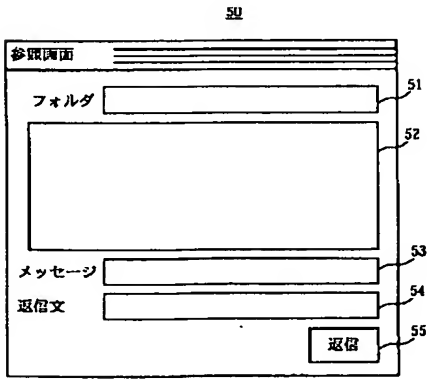
【図４】



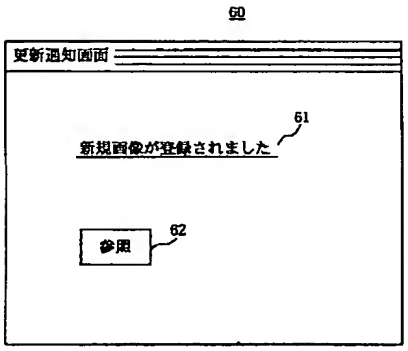
【図６】



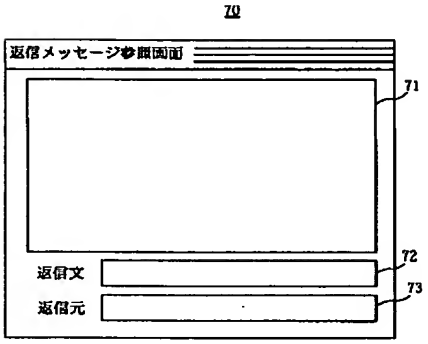
【図８】



【図９】



【図１０】



【図１２】

端末装置		フォルダ					
名称	タイプ	共用	パパ	ママ	太郎	次郎	花子
パーソナルコンピュータ	フリー	A	B	B	B	B	B
テレビ受像機	チェック	A	B	B	B	B	B
携帯電話	チェック	B	C	C	C	C	C

フロントページの続き

(72)発明者　藤井　巌
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内
(72)発明者　藤野　勤
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内
(72)発明者　高野　万滋
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内
(72)発明者　遠山　大雪
大阪府大阪市中央区安土町二丁目３番13号
大阪国際ビル　ミノルタ株式会社内

Ｆターム(参考)　5C025 BA27 CA02 CA09 CB10 DA05
5C064 BA01 BB10 BC18 BC23 BC25
BD02 BD08

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-171510

(43)Date of publication of application : 14.06.2002

---

(51)Int.Cl. H04N 7/173

H04N 5/44

---

(21)Application number : 2000-367832 (71)Applicant : MINOLTA CO LTD

(22)Date of filing : 01.12.2000 (72)Inventor : HARA YOSHIHIRO

DEYAMA HIROYUKI

FUJII IWAO

FUJINO TSUTOMU

TAKANO KAZUSHIGE

TOOYAMA DAISETSU

---

(54) IMAGE SERVER UNIT AND IMAGE COMMUNICATION SYSTEM EMPLOYING THE IMAGE SERVER UNIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image communication system that automatically informs terminals within a required range about the storage of the digital image when a digital image is stored in a server unit.

SOLUTION: In the image communication system where the image server 4 provided with a storage device having storage areas to store image data and terminals 2, 5, 7 are interconnected through a network, the image server 4 is provided with the storage device that has at least one storage area to store image data, a storage request reception means that receives a storage request to request storage of image data to the storage device and including area designation to designate the storage area storing the image data from a data

providing terminal, a write means that writes the image data to a storage area designated by the area designation, a destination decision means that decides a display terminal acting like a destination of a storage notice, which the destination decision means informs of a fact of storing the image data, by using the area designation, and a storage notice means that transmits the storage notice to the destination decided by the destination decision means.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is a network connection system equipped with the network connection equipment for connecting to an external network the internal network which has two or more computers, and this internal network. An end is connected to said internal network and, as for said network connection

equipment, the other end is connected to said external network. The switching means which changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, and when predetermined conditions are satisfied The network connection system characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[Claim 2] The network connection system according to claim 1 characterized by having further the fire wall which checks access to said internal network from said external network, and restricts access to an internal network between said internal networks and said external networks when this access is unlawful access.

[Claim 3] Said internal network and said external network It connects through the fire wall including an alarm generating means to generate an alarm when there is unlawful access to said internal network from said external network. It is the network connection system according to claim 1 characterized by realizing said network connection equipment as a function in said fire wall, and said control means making said switching means a substantial cutting condition when said alarm generating means generates an alarm.

[Claim 4] It is network connection equipment for connecting to an external

network the internal network which has two or more computers. The switching means which an end is connected to said internal network, and the other end is connected to said external network, and changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, Network connection equipment characterized by having the control means which changes whether said switching means is made into a substantial connection condition when predetermined conditions are satisfied, or it considers as a substantial cutting condition.

[Claim 5] It is network connection equipment according to claim 4 characterized by realizing said switching means and said control means as a function of a fire wall including an alarm generating means to generate an alarm when there is unlawful access to said internal network from said external network, respectively, and said control means making said switching means a substantial cutting condition when said alarm generating means generates an alarm.

[Claim 6] Said control means is network connection equipment according to claim 4 or 5 characterized by changing whether said switching means is made into a substantial connection condition according to generating of this predetermined event by supervising generating of the predetermined event in said internal network, or it considers as a substantial cutting condition.

[Claim 7] said control means -- a time check -- network connection equipment

given in claim 4 characterized by changing whether said switching means is made into a substantial connection condition when the time amount clocked by the means turns into predetermined time amount, or it considers as a substantial cutting condition thru/or any 1 term of 6.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the network connection system and equipment which connect internal networks, such as LAN (Local Area Network), and external networks, such as WAN (Wide Area Network).

[0002]

[Description of the Prior Art] Although it is increasingly used in a certain form,

carrying out network connection of the computer of recent years many, it has been a big technical problem how unlawful access to each computer is prevented. Especially in the network system to which internal networks, such as LAN, and external networks, such as WAN including the Internet, are connected, generally, the fire wall was prepared between the internal network and the external network, and each computer has prevented being unjustly accessed from an external network by the authentication and filtering by the fire wall.

[0003] However, each computer connected to the internal network also by the network connection system through a fire wall will always be fundamentally connected also with the external network. For this reason, it was impossible to have intercepted unlawful access from an external network completely. Then, in JP,2000-10887,A, the network interface module with a security switch is proposed as a technique for preventing unlawful access from the outside in each computer.

[0004] Drawing 4 is the block diagram showing the network interface module with a security switch of a publication in JP,2000-10887,A. The network interface module 101 is formed by 1 to 1 corresponding to a computer 105, and consists of a network interface 102 and a power-source interface 103 including the security switch 104 so that it may illustrate.

[0005] The power of the network interface module 101 is supplied from the

power source 107 in a computer 105. If CPU106 suspends supply of the power from a power source 107, the security switch 104 will turn off and a network interface 102 will serve as impossible of operation. It becomes impossible to access a computer 105 from an outside network by this, and unlawful access to a computer 105 can be prevented now.

[0006]

[Problem(s) to be Solved by the Invention] However, with the technique of a publication, the network interface module 101 must be formed in JP,2000-10887,A corresponding to each computer 105. However, by the system to which the internal network and the external network were connected, unlawful access to the computer 105 from an internal network can seldom be considered. It is useless from a tooth space and the field of cost to make a redundant configuration each of a computer 105 to such unlawful access that is hardly considered.

[0007] Moreover, if it is in the calculating machine further connected with the internal network in the external network, although an exchange of the data in an internal network is performed frequently, there are usually few exchanges of data with an external network overwhelmingly to this. For this reason, if the network interface module 101 is formed to each of a calculating machine 105 like JP,2000-10887,A and it can be made to carry out access refusal of each of a

calculating machine 105, trouble may arise in an exchange of the data only in an internal network.

[0008] This invention aims at offering the network access system which can exchange the data in an internal network efficiently while it prevents unjust access from an external network to the computer connected to the internal network.

[0009]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the network connection system concerning the 1st viewpoint of this invention It is a network connection system equipped with the network connection equipment for connecting to an external network the internal network which has two or more computers, and this internal network. An end is connected to said internal network and, as for said network connection equipment, the other end is connected to said external network. The switching means which changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, and when predetermined conditions are satisfied It is characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[0010] In the above-mentioned network connection system, when a control

means makes a switching means a substantial cutting condition, access to an internal network from an external network serves as impossible. This becomes possible to intercept unlawful access to an internal network from an external network. Here, even when the switching means is in the substantial cutting condition, the calculating machines in an internal network have kept the connection condition mutual, and trouble does not produce them in an exchange of the data in an internal network.

[0011] Between said internal networks and said external networks, the above-mentioned network connection system checks access to said internal network from said external network, and when this access is unlawful access, it shall be further equipped with the fire wall which restricts access to an internal network.

[0012] In the above-mentioned network connection system, said internal network and said external network may be connected through a fire wall including an alarm generating means to generate an alarm, when there is unlawful access to said internal network from said external network. In this case, said network connection equipment should be realized as a function in said fire wall, and said control means can make said switching means a substantial cutting condition, when said alarm generating means generates an alarm.

[0013] As it ********(ed), by using a fire wall together in addition to a switching

means, unlawful access to an internal network from an external network can be prevented more firmly, and it becomes possible to build a system with still higher security.

[0014] In order to attain the above-mentioned purpose, the network connection equipment concerning the 2nd viewpoint of this invention It is network connection equipment for connecting to an external network the internal network which has two or more computers. The switching means which an end is connected to said internal network, and the other end is connected to said external network, and changes said internal network and said external network to either of a substantial connection condition and a substantial cutting condition, When predetermined conditions are satisfied, it is characterized by having the control means which changes whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition.

[0015] In the above-mentioned network connection equipment, said switching means and said control means may be realized as a function of a fire wall including an alarm generating means to generate an alarm, when there is unlawful access to said internal network from said external network, respectively. In this case, said control means can make said switching means a substantial cutting condition, when said alarm generating means generates an alarm.

[0016] In the above-mentioned network connection equipment, said control

means shall supervise generating of the predetermined event in said internal network, and shall change whether said switching means is made into a substantial connection condition according to generating of this predetermined event, or it considers as a substantial cutting condition again.

[0017] the above-mentioned network connection equipment -- setting -- said control means -- further -- a time check -- when the time amount clocked by the means turns into predetermined time amount, it shall change whether said switching means is made into a substantial connection condition, or it considers as a substantial cutting condition

[0018]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to an accompanying drawing.

[0019] Drawing 1 is the block diagram showing the network connection structure of a system concerning the gestalt of this operation. In this network connection system, two or more computers 11 are connected to LAN1 as an internal network so that it may illustrate. LAN1 is connected to the circuit switch section 21 and a control section 22. The circuit switch section 21 and a control section 22 are contained in the internal network in large semantics. The other end of the circuit switch section 21 is connected to WAN3 as an external network. In addition, if it states concretely, LAN1 can be made into intranet and WAN3 can

be made into the Internet.

[0020] The circuit switch section 21 changes whether between LAN1 and WAN3 is made into a connection condition, or it considers as a cutting condition based on the control signal sent from the control section 22. A control section 22 generates and outputs the control signal which changes the condition of the circuit switch section 21 based on the control signal acquired from LAN1.

[0021] A control section 22 is realizable with the line board linked to LAN1, the personal computer which controls the circuit switch section 21. In this case, the circuit switch section 21 may be a cable switch which carries out ON/OFF of LAN1 and WAN3 physically with a serial signal. Moreover, the hardware of dedication may realize the circuit switch section 21 and a control section 22. In this case, the interface linked to LAN1 and the interface connected to WAN3 should just be offered.

[0022] Hereafter, the actuation in this network connection system is explained. Here, in the usual condition, the circuit switch section 21 shall be in a cutting condition.

[0023] Either of the events 11 which should connect LAN1 with WAN3, for example, a calculating machine, accesses the computer apparatus on WAN3, and when the event which is going to acquire data occurs, the calculating machine 11 concerned notifies the purport which is going to access WAN3 to a

control section 22. A control section 22 changes a control signal to the circuit switch section 21, and makes delivery and the circuit switch section 21 changed to a connection condition based on this notice.

[0024] After the circuit switch section 21 is in a connection condition, the calculating machine 11 concerned accesses the computer apparatus on WAN3, and acquires data from there. After acquisition of data is completed, the computer 11 concerned notifies the purport which ended access to WAN3 to a control section 22. A control section 22 changes a control signal to the circuit switch section 21, and makes delivery and the circuit switch section 21 changed to a cutting condition based on this notice.

[0025] On the other hand, when the computer apparatus on WAN3 tends to access either of the calculating machines 11 in LAN1, since the circuit switch section 21 is in the cutting condition, a calculating machine 11 cannot usually be accessed in fact. Also in this condition, since calculating-machine 11 comrades in LAN1 are in the connection condition, they can exchange data of each other freely.

[0026] As explained above, if the control section 22 makes the circuit switch section 21 the cutting condition, in the network connection system concerning the gestalt of this operation, the computer 11 in LAN1 cannot be accessed from WAN3. For this reason, since what is necessary is just to make the circuit switch

section 21 into the cutting condition altogether when the calculating machine 11 in LAN1 does not need to exchange WAN3 and data as an external network, it can protect being unjustly accessed by the calculating machine 11 in LAN1 from WAN3.

[0027] Moreover, even when the circuit switch section 21 is in a cutting condition, computer 11 comrades in LAN1 can always be maintaining the connection condition. For this reason, trouble does not arise in an exchange of the data of calculating-machine 11 comrades in LAN1, and processing in LAN1 can be performed efficiently.

[0028] This invention is not restricted to the gestalt of the above-mentioned operation, but various deformation and application are possible for it. Hereafter, the strange gestalt of the gestalt of the above-mentioned operation applicable to this invention is explained.

[0029] With the gestalt of the above-mentioned operation, the control section 22 had changed the circuit switch section 21 to the connection condition or the cutting condition based on the event generated in LAN1 which is an internal network. On the other hand, it is possible to change the circuit switch section 21 also according to the event generated in WAN3 which is an external network. But although the event generated in WAN3 is told to a control section 22 only when the circuit switch section 21 is in a connection condition, a control section

22 can change the circuit switch section 21 from a connection condition to a cutting condition to suitable timing based on the event generated in WAN3.

[0030] Moreover, a change in the connection condition of the circuit switch section 21 and cutting condition by the control section 22 can also be carried out by the time amount which a timer clocks. For example, neither synchronous application, mail, delivery of news, transfer of a file nor backup can be performed if it does not necessarily connect always. Then, what is necessary is to make the circuit switch section 21 into a connection condition in the time zone set beforehand according to the time amount which a timer clocks, and just to deliver and receive such data. In addition, although a timer is in the outside of a control section 22 also as that with which control-section 22 the very thing is equipped and enabled the input of a hour entry at the control section 22, it may be any.

[0031] With the gestalt of the above-mentioned operation, LAN1 and WAN3 should be connected through the circuit switch section 21. On the other hand, it is possible to also constitute the network connection system of a configuration of to have used the fire wall together to connection between LAN1 and WAN3.

[0032] Drawing 2 is the block diagram which used the fire wall together and in which showing the network connection structure of a system of other configurations. In this network connection system, the fire wall 23 is further

formed between the circuit switch section 21 and LAN1. But the location of a fire wall 23 may be between the circuit switch section 21 and WAN3.

[0033] Suppose that the computer 11 in LAN1 had unlawful access from WAN3 in the network system of drawing 2 . Here, if the circuit switch section 21 is in the connection condition, the unlawful access will reach even a fire wall 23. Next, although a fire wall 23 filters access from WAN3, since it is unlawful access, it is not told to the computer 11 in LAN1. By such configuration, prevention of unlawful access is strengthened and a system with still higher security can be built rather than the system to the computer 11 in LAN1 from WAN3 shown with the gestalt of the above-mentioned operation.

[0034] Drawing 3 is the block diagram which used the fire wall together and in which showing the network connection structure of a system of other configurations further. In this network connection system, LAN1 and WAN3 are connected through the fire wall 2, and the circuit switch section 21 and a control section 22 are realized as a function of a fire wall 2. The fire wall 2 contains the alarm generating section 24 which emits an alarm, when the computer 11 in LAN1 has unlawful access from WAN3.

[0035] Here, when the alarm generating section 24 generates an alarm, a control section 22 sends a control signal to the circuit switch section 21 so that LAN1 and WAN3 may be in a cutting condition. When there is access to WAN3 from

the computer 11 in LAN1 after the circuit switch section 21 was changed to the cutting condition for example, a control section 22 can send a control signal to the circuit switch section 21 so that it may be in a connection condition again. In addition, a control section 22 can be controlled to change the circuit switch section 21 to a cutting condition, also when various events which were described above occur besides when the alarm generating section 24 generates an alarm.

[0036] Since it not only does not tell the unlawful access as a fire wall 2, but the circuit switch section 21 is made into a cutting condition when there is unjust access from WAN3 to the computer 11 in LAN1, prevention of unlawful access can be strengthened more with having considered as such a configuration. Thereby, a system with still higher security can be built rather than the system shown with the gestalt of the above-mentioned operation.

[0037] With the gestalt of the above-mentioned operation, LAN1 was made into the internal network and the network connection system by which WAN3 as an external network was connected to this was explained as an example. However, the circuit switch section 21 and the control section 22 which described LAN and LAN above or more in any one of LANs of it even in the network system connected with the router etc., for example can be prepared.

[0038]

[Effect of the Invention] As explained above, while being able to prevent unjust

access from an external network to each computer connected to the internal network according to this invention, the data in an internal network can be exchanged convenient.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the network connection structure of a system concerning the gestalt of operation of this invention.

[Drawing 2] It is the block diagram showing the network connection structure of a system concerning the gestalt of other operations of this invention.

[Drawing 3] It is the block diagram showing the network connection structure of a

system concerning the gestalt of other operations of this invention.

[Drawing 4] It is the block diagram showing the network interface module with a security switch concerning the conventional example.

[Description of Notations]

1 LAN

2 Fire Wall

3 WAN

11 Computer

21 Circuit Switch Section

22 Control Section

23 Fire Wall

24 Alarm Generating Section